UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,640	08/25/2003	Hisashi Takayama	4777-31	2508

29540 7590 06/07/2007

DAY PITNEY LLP
7 TIMES SQUARE
NEW YORK, NY 10036-7311

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
06/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/647,640	TAKAYAMA ET AL.	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) *3-6,8,9,14,15,27-30 and 34-39* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7,11-13,19 and 22-24* is/are rejected.

7)☒ Claim(s) *1,2,7,10,12,13,16,19-21,24-26 and 31-33* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Species I in the reply filed on 27 April 2007 is acknowledged.

Claim Objections

2. Claims 1, 2, 7, 10, 12, 13, 16, 19, 20, 21, 24-26, 31-33 are objected to because of the following informalities:

"said" should be deleted from line 5 of claim 1;

"user" should be changed to "said user" in line 6 of claim 1;

"in process" should be changed to "in a process" in line 8 of claim 1;

"user" should be changed to "said user" in line 8 of claim 1;

"authentication side" should be changed to "an authentication side" in line 9 of claim 1;

"user" should be changed to "said user" in line 9 of claim 1;

"a user" should be changed to "said user" in line 10 of claim 1;

"authentication information" should be changed to "said authentication information" in line 11 of claim 1;

"an electronic value" should be changed to "said electronic value" in line 11 of claim 1;

"value authentication information" should be changed to "said value authentication information" in line 13 of claim 1;

"authentication information" should be changed to "said authentication information" in line 15 of claim 1;

"received electronic value" should be changed to "said received electronic value" in line 16 of claim 1;

"value authentication information" should be changed to "said value authentication information" in line 17 of claim 1;

"electronic value" should be changed to "said electronic value" in line 17 of claim 1;

"value authentication information" should be changed to "said value authentication information" in lines 18-19 of claim 1;

"encrypted part" should be changed to "an encrypted part" in line 2 of claim 2;

"value authentication information" should be changed to "said value authentication information" in lines 3 of claim 2;

"master key" should be changed to "a master key" in line 4 of claim 2;

"in process" should be changed to "in said process" in line 5 of claim 2;

"a user" should be changed to "said user" in line 5 of claim 2;

"value authentication" should be changed to "said value authentication" in lines 6 of claim 2;

"a decryption key" should be changed to "said decryption key" in line 10 of claim 2;

"electronic value" should be changed to "an electronic value" in line 2 of claim 7;

"authentication apparatus" should be changed to "an authentication apparatus" in line 8 of claim 7;

"authentication information" should be changed to "said authentication information" in line 9 of claim 7;

"authentication apparatus" should be changed to "said authentication apparatus" in line 10 of claim 7;

"user" should be changed to "said user" in line 11 of claim 7;

"decryption key" should be changed to "a decryption key" in line 2 of claim 10;

"master key" should be changed to "a master key" in line 4 of claim 10;

"value authentication information" should be changed to "said value authentication information" in line 5 of claim 10;

"data" should be changed to "said data" in line 7 of claim 10;

"authentication apparatus" should be changed to "said authentication apparatus" in line 8 of claim 10;

"user" should be changed to "said user" in line 8 of claim 10;

"property" should be changed to "a property" in line 2 of claim 12;

"mobile terminal" should be changed to "a mobile terminal" in line 2 of claim 13;

"electronic value" should be changed to "an electronic value" in line 3 of claim 13;

"encrypted part of electronic value" should be changed to "an encrypted part of said electronic value" in line 4 of claim 13;

"value authentication information" should be changed to "said value authentication information" in line 7 of claim 13;

"random number" should be changed to "said random number" in line 7 of claim 13;

"user" should be changed to "a user" in line 11 on claim 13;

"a decryption key of encrypted part" should be changed to "a decryption for said encrypted part" in line 2 of claim 16;

"value authentication information" should be changed to "said value authentication information" in line 3 of claim 16;

"master key" should be changed to "a master key" in line 4 of claim 16;

"master key" should be changed to "said master key" in line 6 of claim 16;

"a mobile terminal" should be changed to "said mobile terminal" in line 2 of claim 19;

"user" should be changed to "a user" in line 3 of claim 20;

"said first irreversible calculation process" should be changed to "a first irreversible calculation process" in line 6 of claim 20;

"encryption key" should be changed to "an encryption key" in line 6 of claim 20;

"value authentication information" should be changed to "said value authentication information" in line 7 of claim 20;

"master key" should be changed to "a master key" in line 8 of claim 20;

"it" should be changed to "said electronic value" in line 10 of claim 20;

"encryption key" should be changed to "an encryption key" in line 5 of claim 21;

"value authentication information" should be changed to "said value authentication information" in line 6 of claim 21;

"it" should be changed to "said electronic value" in line 9 of claim 21;

"user" should be changed to "said user" in line 2 of claim 24;

"user" should be changed to "said user" in line 4 of claim 24;

"user" should be changed to "a user" in line 1 of claim 25;

"mobile terminal" should be changed to "a mobile terminal" in line 1 of claim 25;

"authentication apparatus" should be changed to "an authentication apparatus" in line 2 of claim 25;

"electronic value issuance server" should be changed to "an electronic value issuance server" in line 2 of claim 25;

"electronic value" should be changed to "an electronic value" in line 3 of claim 25;

"electronic value" should be changed to "said electronic value" in line 6 of claim 25;

"user" should be changed to "said user" in line 7 of claim 25;

"process" should be changed to "a process" in line 8 of claim 25;

"user" should be changed to "said user" in line 8 of claim 25;

"authentication apparatus" should be changed to "said authentication apparatus" in line 9 of claim 25;

"random number" should be changed to "a random number" in line 9 of claim 25;

"it" should be changed to "said random number" in line 9 of claim 25;

"mobile terminal" should be changed to "said mobile terminal" in lines 9-10 of claim 25;

"mobile terminal" should be changed to "said mobile terminal" in line 11 of claim 25;

"electronic value" should be changed to "said electronic value" in line 12 of claim 25;

"user" should be changed to "said user" in line 12 of claim 25;

"value authentication information" should be changed to "said value authentication information" in lines 13-14 of claim 25;

"authentication information" should be changed to "said authentication information" in line 16 of claim 25;

"authentication apparatus" should be changed to "said authentication apparatus" in line 18 of claim 25;

"electronic value" should be changed to "said electronic value" in line 19 of claim 25;

"value authentication information" should be changed to "said value authentication information" in line 20 of claim 25;

"user" should be changed to "said user" in line 19 of claim 25;

"encrypted part" should be changed to "an encrypted part" in line 2 of claim 26;

"value authentication information" should be changed to "said value authentication information" in lines 3 of claim 26;

"master key" should be changed to "a master key" in line 4 of claim 26;

"in process" should be changed to "in said process" in line 5 of claim 26;

"a user" should be changed to "said user" in line 5 of claim 26;

"value authentication" should be changed to "said value authentication" in lines 6 of claim 26;

"a decryption key" should be changed to "said decryption key" in line 10 of claim 26;

"electronic key" should be changed to "an electronic key" in line 2 of claim 31;

"electronic key" should be changed to "said electronic key" in line 2 of claim 31;

"electronic key" should be changed to "said electronic key" in line 3 of claim 31;

"an electronic key" should be changed to "said electronic key" in line 6 of claim 31;

"value authentication information" should be changed to "said authentication information" in lines 6-7 of claim 31 OR, "authentication information" should be changed to "value authentication information" in line 3 of claim 31 and "value

authentication information" should be changed to "said value authentication information" in lines 6-7 of claim 31;

"electronic key" should be changed to "said electronic key" in line 8 of claim 31;

"it" should be changed to "said encryption key" in line 11 of claim 31;

"electronic key" should be changed to "said electronic key" in line 12 of claim 31;

"electronic key" should be changed to "said electronic key" in line 12 of claim 31;

"it" should be changed to "said random number" in line 13 of claim 31;

"value authentication information" should be changed to "said value authentication information" in line 16 of claim 31;

"value authentication information" should be changed to "said value authentication information" in lines 17-18 of claim 31;

"user" should be changed to "said user" in line 21 of claim 31;

"electronic key" should be changed to "said electronic key" in line 2 of claim 32;

"it" should be changed to "said second random number" in line 3 of claim 32;

"mobile terminal" should be changed to "said mobile terminal" in line 3 of claim 32;

"mobile phone" should be changed to "a mobile phone" in line 4 of claim 32;

"user" should be changed to "said user" in line 4 of claim 32;

"electronic key issuance request message" should be changed to "said electronic key issuance request message" in line 6 of claim 32;

"mobile terminal" should be changed to "said mobile terminal" in lines 6-7 of claim 32;

"a fourth irreversible calculation process" should be changed to "said fourth irreversible calculation process" in lines 8-9 of claim 32;

"user" should be changed to "said user" in line 11 of claim 32;

"an electronic key" should be changed to "said electronic key" in line 11 of claim 32;

"electronic key" should be changed to "said electronic key" in line 3 of claim 33;

"electronic key" should be changed to "said electronic key" in line 3 of claim 33;

"key ID" should be changed to "said key ID stored" in line 4 of claim 33;

Appropriate correction is required.

Examiner notes that claim line numbers correspond to claims submitted on 25 August 2003.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 7, 11-13, 19, 22-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 7 does not clearly define the function G, which renders the claim indefinite.

Claim 7 recites, "encoding by an irreversible calculation process (F) on data," which renders the claim indefinite because it is unclear what 'data' is being encoded by process F. The result of encoding process (F) is value authentication information (F(VPW')). So shouldn't the encoding process (F) be performed on authentication information (VPW), defined previously?

Claims 11, 12 recite, "attribute information set with respect to each electronic value with said electronic value," which renders the claims indefinite because it is unclear how the attribute information is set with respect to electronic values.

Claim 13 does not clearly define the function F, which renders the claim indefinite.

Claim 19 recites the limitation "authentication process" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "electronic value secret information" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 22 recites the limitation "signature information" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 23 recites the limitation "signature information" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Claim 24 recites the limitation "result of risk evaluation" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Allowable Subject Matter

5. Claims 1, 2, 7, 10-13, 16-26, 31-33 would be allowable if rewritten or amended to overcome the objections and the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

6. The following is an examiner's statement of reasons for allowance: The claimed invention generally concerns user authentication wherein the authentication side transmits a random number to the user. The user hashes an authentication value with a first one-way hash function and encrypts the hash. The user then concatenates the encrypted hash with the received random number and hashes the concatenation with a second one-way hash function to be transmitted to the authentication side along with the encrypted hash. The authentication side then decrypts the received hash, concatenates the decrypted hash with the random number that was

previously transmitted to the user in question, hashes the concatenation with the second one-way hash function, and compares the hashed concatenation with the hashed concatenation received form the user. If the authentication side verifies that the hashes are identical, the user is authenticated.

7. The closes prior art (Larsen, U.S. Publication No. 2004/0098627) discloses a similar user authentication system wherein the authentication side transmits a random number to the user (Figure 13, 340). The user concatenates the received random number with a password (Figure 13, 344), hashes the concatenation (Figure 13, 344), and transmits the hash to the authentication side (Figure 13, 346). The authentication side then retrieves the previously transmitted random number (Figure 13, 350), the password associated with the user (Figure 13, 352), concatenates the random number and the password (Figure 13, 354), hashes the concatenation (Figure 13, 354), and compares the hash value with the hash received from the user (Figure 13, 356). If the hashes match, then the user is authenticated (Figure 13, 360).

8. The prior art does not disclose or make obvious hashing the password with a first one-way hash function prior to being concatenated with the received random number and hashed with a second one-way hash function. The prior art also does not disclose or make obvious that this concatenated hash is transmitted to the authentication side along with the encrypted first hash such that the authentication side decrypts the encrypted hash, concatenates the decrypted hash with the previously transmitted random number, hashes the concatenation with the second one-way hash function, and compares the hashed concatenation with the hashed concatenation received from the user in order to authentication the user.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kaufman, U.S. Patent No. 5,418,854

Kaufman, U.S. Patent No. 6,178,508

Brickell, U.S. Patent No. 6,834,112

Chida, U.S. Patent No. 6,938,012

Hansen, U.S. Publication No. 2003/0021419

Larsen, U.S. Publication No. 2004/0098627

Axelsson, U.S. Publication No. 2005/0204142

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin E. Lanier